UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/879,575	06/12/2001	James Alexander Reeds III	037-0039	4755

52218 7590 05/15/2007
ZAGORIN O'BRIEN GRAHAM LLP (037)
7600B NORTH CAPITAL OF TEXAS HIGHWAY
SUITE 350
AUSTIN, TX 78731-1191

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
05/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 09/879,575	Applicant(s) REEDS ET AL.	
	Examiner Ellen C. Tran	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-16,18-22,26-35,37-43 and 45-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5-16, 18-22, 26-35, 37-43, and 45-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ellen Tran

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: filed on 16 February 2007 with acknowledgement of an original application filed on 12 June 2001.

2. Claims 1-3, 5-16, 18-22, 26-35, 37-43, and 45-57 are currently pending in this application. Claims 1, 14, 33, 41, 48, 49, and 53 are independent claims; claim 26 has been amended; claims 4, 17, 23-25,36, and 44 have been cancelled, claim 57 is new. Amendments to the claims are accepted.

3. The replacement sheet of FIG. 4, submitted on 23 August 2006 is accepted.

Response to Arguments

4. In response to Applicant's arguments concerning the 35 U.S.C. § 112 rejection to claims 4, 17, 25-32, 36, and 44, the rejection is withdrawn due to Applicant's amendment canceling the claims.

5. In response to Applicant's concerning the prior art rejection these arguments have been fully considered but they are not persuasive where noted below or moot due to new grounds of rejection, see detailed rejection below.

In response to Applicant's argument beginning on page 12, *"Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fail to teach or suggest selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet"*. The Examiner disagrees with argument paragraphs [0033-0035] of Medvinsky discloses this feature. The continuous decryption key stream is known in the art as the steam cipher. The selecting of a fixed length segment is also well know in the art when using a stream cipher as selecting the key, see Bruce Schneier page

197, 9.4. In addition Medvinsky teaches that the key selected is indexed (i.e. selected) based on the RTP of the packet. Also Medvinsky teaches the RTP as dealing with the session time (i.e. count) of the received or sent packet. Note the Examiner has changed the previous rejection so that the 35 U.S.C. § 103 (a) is now Schneier in view of Medvinsky.

In response to Applicant's argument beginning on page 13, *"Regarding claim 20, Applicants respectfully maintaing that Medvinsky, alone or in combination with Weidong or other references of record, fails to teach or suggest forming the at least a portion of the message digest value by truncating the message digest value".* The Examiner disagrees paragraph [0054] of Medvinsky discloses a packet size change this is interpretted to be equivalent to truncating or expanding. Note the MAC (Message Authentication Code) is considered equivalent to the message digest value, as disclosed in Schneier the on page 435 section 18.4 and page 455 section 18.14, both message digest and MAC are a message authentication formed by a one-way hash functions.

In response to Applicant's argument beginning on page 16, *"Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fail to teach or suggest selecting a fixed length segment of a continuous encryption key stream ... Regarding claim 41, Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or tother references of record, fail to teach or suggest an encrption engine confiugred to apply a portion of a fixed length secgment of a continuous encryption key stream to data to form an encrypted payload".* The Examiner disagrees with argument paragraphs [0033-0035] of Medvinsky discloses this feature. The continuous encryption/decryption key stream is known in the art as the stream cipher. The selecting of a fixed length segment is also well know

in the art when using a stream cipher as selecting the key, see Bruce Schneier page 197, section 9.4. In addition Medvinsky teaches that the key selected is index (i.e. selected) based on the RTP of the packet. Also Medvinsky teaches the RTP as dealing with the session time (i.e. count) of the received or sent packet. Note the Examiner has changed the previous rejection so that the 35 U.S.C. § 103 (a) is now Schneier in view of Medvinsky.

In response to Applicant's argument beginning on page 19, *"Regarding claim 53, Applicants respectfully maintain that Medvinsky, alone or in combination with Weidong or other references of record, fail to teach or suggest selecting a fixed length segment of a continuous encryption key stream based on a received session count of a data packet".* The Examiner disagrees with argument paragraphs [0033-0035] of Medvinsky discloses this feature. The continuous decryption key stream is known in the art as the steam cipher. The selecting of a fixed length segment is also well know in the art when using a stream cipher as selecting the key, see Bruce Schneier page 197, 9.4. In addition Medvinsky teaches that the key selected is index (i.e. selected) based on the RTP of the packet. Also Medvinsky teaches the RTP as dealing with the session time (i.e. count) of the received or sent packet. Note the Examiner has changed the previous rejection so that the 35 U.S.C. § 103 (a) is now Schneier in view of Medvinsky.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1-3, 5, 6, 14-16, 18-22, 41-43, and 45-47,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Applied Cryptography Protocols, Algorithms, and Source Code in C by Bruce Schneier (hereinafter Schneier) in view of Medvinsky U.S. Patent Application Publication No. 2002/0094081 (hereinafter '081).

As to independent claim 1, "and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet" is taught in Schneier teaches stream ciphers utilize keystream generators to encrypt and decrypt packets in section 9.4 on page 197;

the following is not explicitly taught in Schneier:

"A method comprising: selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet" however '081 teaches a stream cipher is utilized that utilizes an RTP time stamp, note the RTP time stamp is the session count on page 3, paragraphs 0033-0035.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers taught in Schneier to include a means to select the encryption key based on the session count. One of ordinary skill in the art would have been motivated to perform such a modification because there is a need to resolve prior art problems for delivering packets over and IP network see '081 (pages 1-2, paragraphs 0013-0015). "Conventional techniques have been specified so that the time stamp continues to be a multiple of the new frame size after an audio change. One such technique is providing a formula for adjusting the timestamp, wherein an adjustment value is added to the time stamp in order to adjust the RC4 key stream. However, the adjustment value added to the time stamp depends on

exactly which audio frame is being processed when the CODEC change is discovered ... there is no guarantee that the two communicating endpoints will be notified (by their Call Agent) of the CODEC change at exactly the same time. Thus, a high probability exists that after the CODEC change the two MTAs would loose synchronization on their RC4 key streams and all RTP packets would not be decrypted. A further problem relates to the receipt of identical RTP session synchronization source (SSRC) identifiers by a gateway terminating several voice connections ... Herein lies a problem similar to the above CODEC change problem. The sequence numbers and the timestamp sequence are both re-initialized which causes the re-use of portions of the previously used key stream and re-start with the same initial timestamp value. Therefore, there is a need to resolve the aforementioned problem relating to the conventional approach for securely delivering voice packets over an IP network".

As to dependent claim 2, "wherein the applying comprises performing a bit per bit streaming decryption process" is taught in Schneier on page 197.

As to dependent claim 3, "wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet" is taught in Schneier on page 197.

As to dependent claim 5, "further comprising: receiving the data packet, the data packet comprising at least a portion of the received session count" however '081 teaches the RTP packets exchanged use at least a portion of the key stream on page 2, paragraphs 0017-0018. The motivation to combine Schneier and '081 is the same as stated in claim 1.

As to dependent claim 6, "wherein the data packet further comprise at least a portion of a received message digest value" is however '081 teaches a MAC is appended to the packet, on page 4, paragraph 0054. In addition, the MAC (Message Authentication Code) is considered equivalent to the message digest value, as disclosed in Schneier the on page 435 section 18.4 and page 455 section 18.14, both message digest and MAC are a message authentication formed by a one-way hash functions. The motivation to combine Schneier and '081 is the same as stated in claim 1.

As to independent claim 14, "A method of generating an encrypted data packet, the method comprising: selecting a fixed length segment of a continuous encryption key stream; applying a portion of the fixed length segment to data to form an encrypted payload" is taught in Schneier page 197, section 9.4, note the continuous encryption/decryption key stream is known in the art as the stream cipher. The selecting of a fixed length segment is also well know in the art when using a stream cipher as selecting the key;

the following is not explicitly taught in Schneier:

"generating a session count based in accordance with the fixed length segment; and" however '081 teaches a stream cipher is utilized that utilizes an RTP time stamp, note the RTP time stamp is the session count on page 3, paragraphs 0033-0035;

"combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet" however '081 teaches the RTP packets exchanged use at least a portion of the key stream on page 2, paragraphs 0017-0018.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers taught in Schneier to include a means to

select the encryption key based on the session count. One of ordinary skill in the art would have been motivated to perform such a modification because there is a need to resolve prior art problems for delivering packets over and IP network see '081 (pages 1-2, paragraphs 0013-0015). "Conventional techniques have been specified so that the time stamp continues to be a multiple of the new frame size after an audio change. One such technique is providing a formula for adjusting the timestamp, wherein an adjustment value is added to the time stamp in order to adjust the RC4 key stream. However, the adjustment value added to the time stamp depends on exactly which audio frame is being processed when the CODEC change is discovered … there is no guarantee that the two communicating endpoints will be notified (by their Call Agent) of the CODEC change at exactly the same time. Thus, a high probability exists that after the CODEC change the two MTAs would loose synchronization on their RC4 key streams and all RTP packets would not be decrypted. A further problem relates to the receipt of identical RTP session synchronization source (SSRC) identifiers by a gateway terminating several voice connections … Herein lies a problem similar to the above CODEC change problem. The sequence numbers and the timestamp sequence are both re-initialized which causes the re-use of portions of the previously used key stream and re-start with the same initial timestamp value. Therefore, there is a need to resolve the aforementioned problem relating to the conventional approach for securely delivering voice packets over an IP network".

As to dependent claims 15 and 16, these claims contain substantially similar subject matter as claims 2 and 3; therefore they are rejected along the same rationale.

As to dependent claim 18, "further comprising: generating a message digest value; and combining at least a portion of the message digest value with the encrypted payload to

form the encrypted data packet" is however '081 teaches a MAC is appended to the packet, on page 4, paragraphs 0054-0055. In addition, the MAC (Message Authentication Code) is considered equivalent to the message digest value, as disclosed in Schneier the on page 435 section 18.4 and page 455 section 18.14, both message digest and MAC are a message authentication formed by a one-way hash functions. The motivation to combine Schneier and '081 is the same as stated in claim 14.

As to dependent claim 19, "wherein the generating comprises: generating the message digest value based on the encrypted payload, the session count and a message digest key" however '081 teaches this limitation on page 4, paragraphs 0054 –0055. The motivation to combine Schneier and '081 is the same as stated in claim 14.

As to dependent claim 20, "further comprising: forming the at least a portion of the message digest value by truncating the message digest value" however '081 teaches this limitation onpage 4, paragraphs 0054 –0055. The motivation to combine Schneier and '081 is the same as stated in claim 14.

As to dependent claim 21, "further comprising transmitting the encrypted data packet to a receiver through a communication channel" however '081 teaches this limitation on page 2, paragraph 0016. The motivation to combine Schneier and '081 is the same as stated in claim 14.

As to dependent claim 22, "further comprising: receiving a received data packet corresponding to the encrypted data packet, the received data packet comprising the encrypted payload, at least a portion of a received session count and a received truncated message digest value; selecting a fixed length segment of a continuous decryption key

stream based on a received session count of a data packet; and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet" however '081 teaches this limitation on page 4, paragraphs 0054 –0055. The motivation to combine Schneier and '081 is the same as stated in claim 14.

As to independent claim 41, this claim is directed to a transmitter of the method of claim 14; therefore it is rejected along similar rationale.

As to dependent claims 42-51, these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 49, "and applying a portion of the fixed length segment by performing a bit per bit streaming decryption to decrypt a payload of the data packet" is taught in Schneier teaches stream ciphers utilize keystream generators to encrypt and decrypt packets in section 9.4 on page 197;

the following is not explicitly taught in Schneier:

"A method comprising: receiving a data packet through a communication channel the data packet comprising at least a portion of a session count; selecting a fixed length segment of a continuous decryption key stream based on the session count" however '081 teaches a stream cipher is utilized that utilizes an RTP time stamp, note the RTP time stamp is the session count on page 3, paragraphs 0033-0035.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers taught in Schneier to include a means to select the encryption key based on the session count. One of ordinary skill in the art would have been motivated to perform such a modification because there is a need to resolve prior art

problems for delivering packets over and IP network see '081 (pages 1-2, paragraphs 0013-0015). "Conventional techniques have been specified so that the time stamp continues to be a multiple of the new frame size after an audio change. One such technique is providing a formula for adjusting the timestamp, wherein an adjustment value is added to the time stamp in order to adjust the RC4 key stream. However, the adjustment value added to the time stamp depends on exactly which audio frame is being processed when the CODEC change is discovered … there is no guarantee that the two communicating endpoints will be notified (by their Call Agent) of the CODEC change at exactly the same time. Thus, a high probability exists that after the CODEC change the two MTAs would loose synchronization on their RC4 key streams and all RTP packets would not be decrypted. A further problem relates to the receipt of identical RTP session synchronization source (SSRC) identifiers by a gateway terminating several voice connections … Herein lies a problem similar to the above CODEC change problem. The sequence numbers and the timestamp sequence are both re-initialized which causes the re-use of portions of the previously used key stream and re-start with the same initial timestamp value. Therefore, there is a need to resolve the aforementioned problem relating to the conventional approach for securely delivering voice packets over an IP network".

As to independent claim 53, **"A method of generating an encrypted data packet, the method comprising: selecting fixed length segment of a continuous encryption key stream; applying a portion of the fixed length segment to data by performing a bit per bit streaming encryption process to form an encrypted payload"** is taught in Schneier teaches stream ciphers utilize keystream generators to encrypt and decrypt packets in section 9.4 on page 197;

the following is not taught in Schneier:

"generating a session count in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet" however '081 teaches a stream cipher is utilized that utilizes an RTP time stamp, note the RTP time stamp is the session count on page 3, paragraphs 0033-0035.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers taught in Schneier to include a means to select the encryption key based on the session count. One of ordinary skill in the art would have been motivated to perform such a modification because there is a need to resolve prior art problems for delivering packets over and IP network see '081 (pages 1-2, paragraphs 0013-0015). "Conventional techniques have been specified so that the time stamp continues to be a multiple of the new frame size after an audio change. One such technique is providing a formula for adjusting the timestamp, wherein an adjustment value is added to the time stamp in order to adjust the RC4 key stream. However, the adjustment value added to the time stamp depends on exactly which audio frame is being processed when the CODEC change is discovered … there is no guarantee that the two communicating endpoints will be notified (by their Call Agent) of the CODEC change at exactly the same time. Thus, a high probability exists that after the CODEC change the two MTAs would loose synchronization on their RC4 key streams and all RTP packets would not be decrypted. A further problem relates to the receipt of identical RTP session synchronization source (SSRC) identifiers by a gateway terminating several voice connections … Herein lies a problem similar to the above CODEC change problem. The sequence numbers and the timestamp sequence are both re-initialized which causes the re-use of

portions of the previously used key stream and re-start with the same initial timestamp value. Therefore, there is a need to resolve the aforementioned problem relating to the conventional approach for securely delivering voice packets over an IP network".

8. **Claims 7-13, 26-35, 37-40, and 48-51,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Applied Cryptography Protocols, Algorithms, and Source Code in C by Bruce Schneier (hereinafter Schneier) in view of Jung U.S. Patent Application Publication No. 2001/0052072 (hereinafter '072).

As to independent claim 33, "and a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet" is taught in Schneier teaches stream ciphers utilize keystream generators to encrypt and decrypt packets in section 9.4 on page 197;

the following is not explicitly taught in Schneier:

"A receiver comprising: a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold" however '072 teaches that the sequence number may be used to synchronize encryption, note the Examiner interprets this synchronization equivalent to 'if a difference between the received session count'.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers over the Internet taught in Schneier to include a means to selecting the encryption key based on if the difference is less than a threshold value. One of ordinary skill in the art would have been motivated to perform such a modification

because there is a requirement of stream encryption algorithms is that the transmitting side and the receiving side be synchronized see '072 (pages 1, paragraphs 0013). "A requirement of stream encryption algorithms is that the transmitting side and the receiving side be synchronized in order for the encryption and decryption to work properly. Specifically, the data must be decrypted in the same order or sequence in which it was encrypted. However, such synchronization is not only difficult to employ and maintain in the IP network 10, but can also consume a significant amount of bandwidth (e.g., 7-10% using RTP)".

9. **Claims 7-13, 26-32, 34, 35, 37-40, and 48-51,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Applied Cryptography Protocols, Algorithms, and Source Code in C by Bruce Schneier (hereinafter Schneier) in view of Medvinsky. U.S. Patent Application Publication No. 2002/0094081 (hereinafter '081) in further view of Jung U.S. Patent Application Publication No. 2001/0052072 (hereinafter '072).

As to dependent claim 7, the following is not explicitly taught in the combination of teaching of Schneier and '081: **"wherein the selecting comprises: selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value"** however '072 teaches that the sequence number may be used to synchronize encryption, note the Examiner interprets this synchronization equivalent to 'if a difference between the received session count'.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers over the Internet taught in Schneier and '081 to include a means to selecting the encryption key based on if the difference is less than a threshold value. One of ordinary skill in the art would have been motivated to perform such a

modification because there is a requirement of stream encryption algorithms is that the transmitting side and the receiving side be synchronized see '072 (pages 1, paragraphs 0013). "A requirement of stream encryption algorithms is that the transmitting side and the receiving side be synchronized in order for the encryption and decryption to work properly. Specifically, the data must be decrypted in the same order or sequence in which it was encrypted. However, such synchronization is not only difficult to employ and maintain in the IP network 10, but can also consume a significant amount of bandwidth (e.g., 7-10% using RTP)".

As to dependent claim 8, "wherein the selecting further comprises: extracting the at least a portion of the received session count from the encrypted data packet; expanding the at least a portion of the received session count to the received session count; and comparing the received session count to the locally generated session count" is disclosed in '081 page 4 paragraph 0054.

As to dependent claim 9, "further comprising: discarding the data packet if the difference is not less than the threshold value" however '072 teaches an error detection mechanism is used to detect when the synchronization is lost on page 1, paragraph 0015. Note if the packet is lost it is equivalent to discarded.

As to dependent claim 10, "further comprising: re-synchronizing a decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the difference is not less than the threshold value" however '072 teaches an error message may initiate a data recovery procedure on page 2, paragraph 0030.

As to dependent claim 11, "further comprising: discarding the data packet if the at least a portion of the received message digest value does not match a locally generated

message digest value" however '072 teaches an error detection mechanism is used to detect when the synchronization is lost on page 1, paragraph 0015. Note if the packet is lost it is equivalent to discarded.

As to dependent claim 12, "further comprising: re-synchronizing the decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value" is shown in '081 page 4, paragraph 4-5, paragraphs 0054-0057 "In a further embodiment, the above solution is employed for a MAC (Message Authentication Code) algorithm change, resulting in a packet size change. Traditionally, for convenience the same RC4 key stream may be used in the generation of the keying material needed to calculate a MAC for each packet (a MAC is appended after the encrypted text). Where the MAC pad is key used to generate the MAC, for one-time use only. So, where a key stream is used for MAC generation (instead of or in addition to encryption) and the size of that random pad changes, one must rekey and start a new RC4 key stream in the same way as for CODE changes".

As to dependent claim 13, "further comprising: extracting the at least a portion of the received message digest value from the data packet; generating the locally generated message digest value based on the at least a portion of the received session count, a received encrypted payload of the data packet and a message digest key; truncating the locally generated message digest value to form a truncated message digest; and comparing the truncated message digest to the at least a portion of the received message digest value" is shown in '081 page 4, paragraph 4-5, paragraphs 0054-0057.

As to dependent claims 26-32, these claims contain substantially similar subject matter as claims 7-13; therefore they are rejected along the same rationale.

As to dependent claims 34, 35, 37-39 these claims contain substantially similar subject matter as claims 2, 3, 5-8; therefore they are rejected along the same rationale.

As to dependent claim 40, "further comprising: a message digest extractor configured to extract the at least a portion of the received message digest value from the received encrypted data packet" is taught in '081 page 4, paragraph 0054 "In a further embodiment, the above solution is employed for a MAC (message Authentication Code) algorithm change, resulting a in a packet size change";

"a message digest generator configured to generate a locally generated message digest value based on the at least a portion of the session count, a received encrypted payload of the data packet and a message digest key" is shown in '081 pages 4-5 paragraph 0055-0056 "For example, additional key stream bytes may be allocated to calculate a MAC for each frame. However, ehre is only one MAC needed for the whole RTP packet and if an RTP packet contains multiple frames only the key stream bytes allocated to one of the frames ... Where the MAC pad is a key used to generate the MAC, for one-time use only;

"a truncator configured to truncate the locally generated message digest value to form a truncated message digest; and a message digest evaluator configured to compare the truncated message digest value to the at least a portion of the received message digest value" is disclosed in '081 page 5, paragraph 0057 "one must rekey and start a new RC4 key stream in the same way as fro CODEC changes";

"where the received is configured to discard the received encrypted data packed it the truncated message digest value does not match the at least a portion of the received message digest value" is taught in '546 col. 10, lines 1-30 "The key check block is sent to the receiver as a header of the current encrypted data payload. The receiver also retains the last eight bytes of the current packet, it decrypted the first eight bytes (the key check block) and compares the result to the retained last eight bytes ... If there is no match, an error occurred and the receiver takes appropriate action". The motivation to combine references '081 and '546 is the same as stated above in claim 9.

As to independent claim 48, is directed to a system consisting of independent claims 33 and 41; therefore it is rejected along the same rationale.

As to dependent claims 50-52, these claims contain substantially similar subject matter as claims 7-9; therefore they are rejected along the same rationale.

10. **Claims 54-57,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Applied Cryptography Protocols, Algorithms, and Source Code in C by Bruce Schneier (hereinafter Schneier) in view of Medvinsky U.S. Patent Application Publication No. 2002/0094081 (hereinafter '081) in further view of Jung U.S. Patent Application Publication No. 2001/0052072 (hereinafter '072) in further view of Sengodan et al. U.S. Patent 6,918,034 (hereinafter '034).

As to dependent claim 54, the following is not explicitly taught in the combination of teachings of Schneier, '081, and '072: **"further comprising: padding the payload to a given size with padding, the given size corresponding to the fixed length segment size, wherein the fixed length segment of the continuous decryption key is applied to the padded payload, a remaining**

portion of the fixed length segment being applied to the padding" however '034 teaches that padding is added to packets so that each packet is a predetermined block size in col. 4, lines 30-36.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers over the Internet taught in Schneier, '081, and '072 to include a means add padding to the exchanged packets. One of ordinary skill in the art would have been motivated to perform such a modification because there is a need to introduce padding at the packet level see '034 (col. 3, line 65 through col. 4, line 29). "Currently, there exist mechanisms for providing encryption at the IP level and at the RTP level. These mechanisms have taken into account the fact that block encryption schemes require the input to be an integral multiple of the block size. This has been made possible by suitable padding schemes. However, in an environment where several mini-packets are multiplexed into an TRP packet, no suitable encryption (and corresponding padding) mechanism has been proposed … It can be seen then that there is a need to provide padding and encryption on a mini-packet basis. It can also be seen that there is a need for a mechanism to perform padding and encryption at the mini-packet level. It can also be seen then that there is a need for a mechanism to perform authentication at the mini-packet level. To overcome the limitations in the prior art described above, and to overcome other limitations that will become apparent upon reading and understanding the present specification, the present invention discloses a method and apparatus to provide encryption and authentication of a mini-packet in a multiplexed real time protocol (RTP) payload. The present invention solves the above-described problems by providing a mechanism to perform padding, encryption and authentication at the mini-packet level".

As to dependent claim 55, "further comprising: padding the data with padding; applying the fixed length segment to the padded data to form padded encrypted data, wherein a remaining portion of the fixed length segment is applied to the padding; and de-padding the padded encrypted data to form the encrypted payload" however '034 teaches how the padding is added and removed (de-padding) to authenticate and encryption of packets exchanged in col. 4, lines 30-61.

As to dependent claim 56, "further comprising: a padding engine operable to pad the data and coupled to supply the padded data to the encryption engine; and a pad remover coupled to receive encrypted padded data from the encryption engine and operable to remove the encrypted padding" however '034 teaches how the padding is added and removed (de-padding) to authenticate and encryption of packets exchanged in col. 4, lines 30-61.

As to dependent claim 57, this claim contains substantially similar subject matter as claim 56; therefore it is rejected along similar rationale.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 8:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
2 May 2007